**IBM Security Identity Governance**

**And Intelligence**

**IGI Rule Management Lab (Lab06)**

**5.2.x**

**David Kuehr-McLaren**

Version 0.3

August 2017

**Document Purpose**

This document provides the instructions for running the IGI Rule Management Lab.

For any comments/corrections, please contact David Edwards ([davidedw@au1.ibm.com)](mailto:davidedw@au1.ibm.com)).

**Document Conventions**

The following conventions are used in this document:

* A step to be performed by the student.

A note, some special information or warning.

A piece of code

Normal paragraph font is used for general information.

The term “IGI” is used to refer to IBM Security Identity Governance and Intelligence.

**Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Release Date** | **Version** | **Authors** | **Comments** |
| 04 Apr 2017 | 0.1 | David Kuehr-McLaren | Initial version |
| 8 Aug 2017 | 0.2 | David Edwards | Check/update for 5.2.3 and Trg Env v4 |
| 26 Oct 2017 | 0.3 | David Edwards | Update for issue when Lab07 is run first |

**Table of Contents**

[1 Introduction to the Lab 4](#_Toc490041219)

[2 Lab Pre-Requisites 5](#_Toc490041220)

[2.1 Expected Knowledge 5](#_Toc490041221)

[2.2 Standard Lab Setup 5](#_Toc490041222)

[2.3 Additional Lab Setup 5](#_Toc490041223)

[3 Lab Instructions 6](#_Toc490041224)

[3.1 Part 1 – Change Parameters of a Task for Development and Test 6](#_Toc490041225)

[3.1.1 Change Task and Job Parameters 6](#_Toc490041226)

[3.2 Part 2 – Create, Compile, and Deploy a New Rule 8](#_Toc490041227)

[3.2.1 Creating a new rule as part of the Live Event rule flow of the In Event Queue 8](#_Toc490041228)

[3.2.2 Creating a New Rule 10](#_Toc490041229)

[3.2.3 Deploying the new rule as part of the rule flow 13](#_Toc490041230)

[3.3 Create a new user using the “New Hire” process 15](#_Toc490041231)

[3.3.1 Manager creates and new user using the Service Center 15](#_Toc490041232)

[Notices 17](#_Toc490041233)

# Introduction to the Lab

There are several points in the IGI product where custom Java Rules can be applied to change the data and perform custom operations. This lab demonstrates how to set the IGI Account expiration date for a user that is created as part of a Create User workflow. Something like this might be useful in a process to create a new contractor employee. where the access to IGI needs to be revoked after a specific time frame.

This lab also introduces the basics of the Task Planner, where scheduled background processes are configured and managed. The Task Planner manages the running of IGI Tasks. A Task is made up of one or more jobs. A job is a discrete piece of work to manage data, business logic, and external services. A job is reusable in multiple tasks. While a task is running, it cannot be changed. A task must be stopped, changed, and restarted to make changes to background processing.

The parts of the lab are:

1. Change the parameters of the RulesEngine Task to change the cache for development and testing
2. Create and new rule, compile it, and deploy it
3. Create and new user and demonstrate the rule execution setting the expiration value of the new user

# Lab Pre-Requisites

This section defines the lab pre-requisites.

## Expected Knowledge

This lab assumes the following knowledge has been acquired before attempting the labs:

* Familiarity with the IGI Administrative Console and Service Center
* Familiarity with applications, accounts, targets, attributes and permissions

This knowledge can be gained via the introductory (Foundation) training.

In addition, from the IGI Deployment Training, you should be familiar with

* Basic concepts of Rules and Rule Flows
* Ability to access and view to the IGI logs for debugging

## Standard Lab Setup

This lab uses the standard IGI training lab. Setup for this lab is described in the document ***Lab00 - IGI Lab Environment Setup Guide***.

These documents describe the standard training environment used for the IGI labs and the steps to prepare for this lab.

## Additional Lab Setup

No additional lab setup is required for this lab.

However, the third part of this lab relies on a new user flow that is shipped with the training image (v4). If you are using the training image and have run Lab 07 (“Lab07 - User Lifecycle Automation”) you will have deleted the new user flow (that presents the “New Hire” tab for DFox). If this is the case, you can go and get a fresh image of the training VM (or restore a snapshot if you’ve taken it). If this is not feasible, you can repeat the steps in Part 02 of Lab 07 to recreate the user create flow. You may also need to enable the user events in the Required Data in the My Requests activity.

# Lab Instructions

## Part 1 – Change Parameters of a Task for Development and Test

This part of the lab will use the Task Planner to change the default cache setting of the **xxx** job of the RulesEngine Task to load and recompile rules every 1 minute, instead of the default two hours. This task will also enable monitoring of the RuleEngine Task.

Changing the cache setting for the RulesEngine will affect the performance of the system. Loading and compiling the rules every minute uses more IO and CPU. Once done with development and testing, the cache setting should be reset to a higher value.

The steps we will follow:

* Stop the RuleEngine task
* Change the RuleEngine Task Parameters
* Start he RuleEngine task

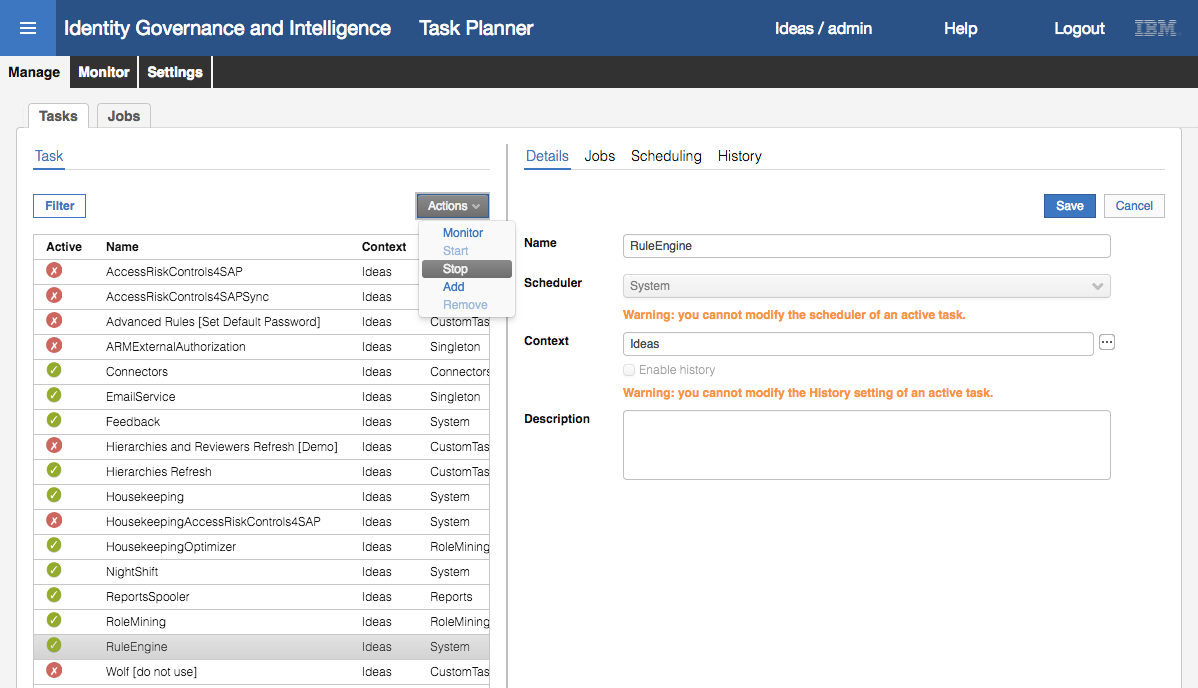
To support this section, you should review the section “Task Planner” in the IGI Knowledge Center (online documentation) at <https://www.ibm.com/support/knowledgecenter/en/SSGHJR_5.2.3/com.ibm.igi.doc/CrossIdeas_Topics/TSKP/manageTimer.html>

### Change Task and Job Parameters

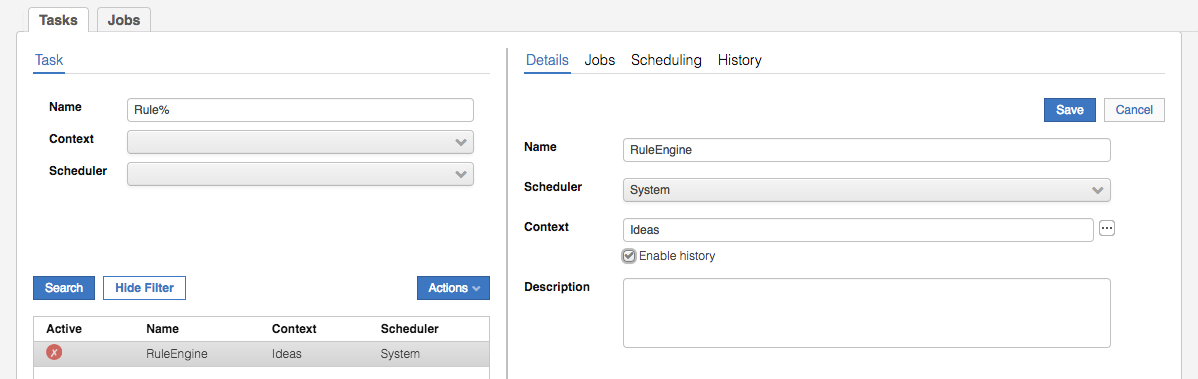
This section will demonstrate how to change the cache parameters of a job. No changes can be done to a task, or the jobs included in a task, while the task is running. The task must be stopped to make changes. In addition to changing the cache time, the lab will also enable monitoring execution of the rules engine, which may help in debugging issues with rule configuration.

The steps are:

* Open the **IGI Administrative Console** (admin/admin)
* Open **Task Planner**
* Select the RuleEngine Task
* Select **Actions > Stop**. The green check next to the name will turn into a red X.

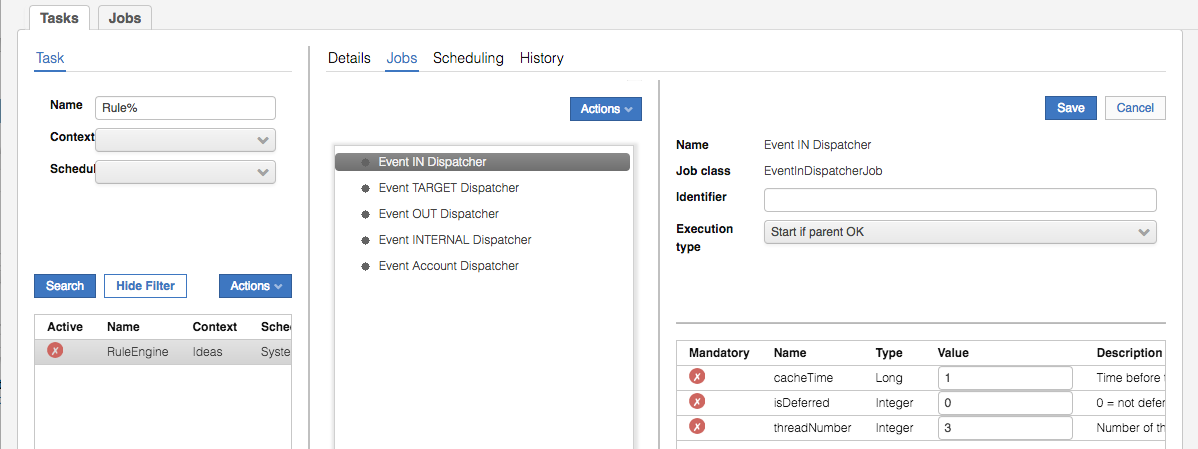


* Highlight the RuleEngine Task
* On the **Details** tab in the right panel, check “Enable history” and click **Save**



A Task is composed of one or more Jobs, usually related in some way. The RuleEngine task is comprised of four jobs, one job for each of the Event Queues, IN User/OU, TGT (Target), OUT, and INTERNAL. Each job has its own parameters. The Rule to be created in the lab will process on the Event IN Queue. By default, the cacheTime parameter is set to 120 minutes, which means that changes made to a rule will not be reloaded and compiled for up to 2 hours. For development and testing the cacheTime is set to 1 minute in order to pick up changes closer to real time.

* Highlight the RuleEngine Task
* Click the **Jobs** tab in the right panel
* Select the “Event IN Dispatcher” Job in the middle pain
* Change the **cacheTime** to “1” minute
* Click **Save** in the right panel



For information, select the “Scheduling” tab and note that the RuleEngine will execute every 20 seconds. Also select the “History” tab and notice that there are no entries in the history table. Start the RuleEngine with the new parameters.

* Select the RuleEngine Task
* Select **Actions > Start** in the left pane. The red X next to the name will turn into a green check.

After 20 seconds, a refresh of the History tab will show an entry showing the success and/or failure of the jobs in the RoleEngine tasks.

The History feature of running tasks will have a slight impact on performance and will consume disk space over a long period time. Once development and debug is complete, it is advisable to disable the history recording of the task.

This completes the changes to the task. Next, we will create and deploy a new Rule.

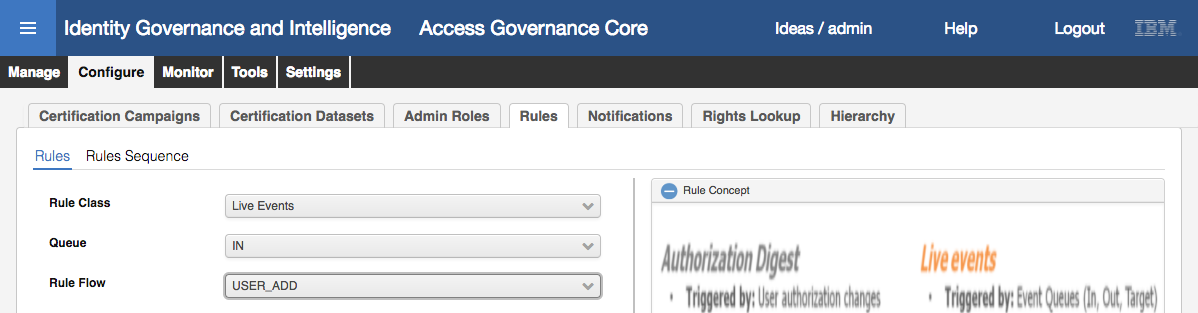
## Part 2 – Create, Compile, and Deploy a New Rule

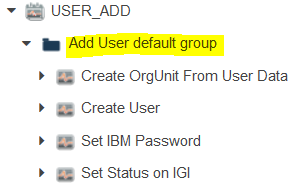
This part of the lab focus on creating a new rule, verifying the rule, and deploying the rule into the rule flow to be executed as part of the RuleEngine scheduled task.

### Creating a new rule as part of the Live Event rule flow of the In Event Queue

Steps:

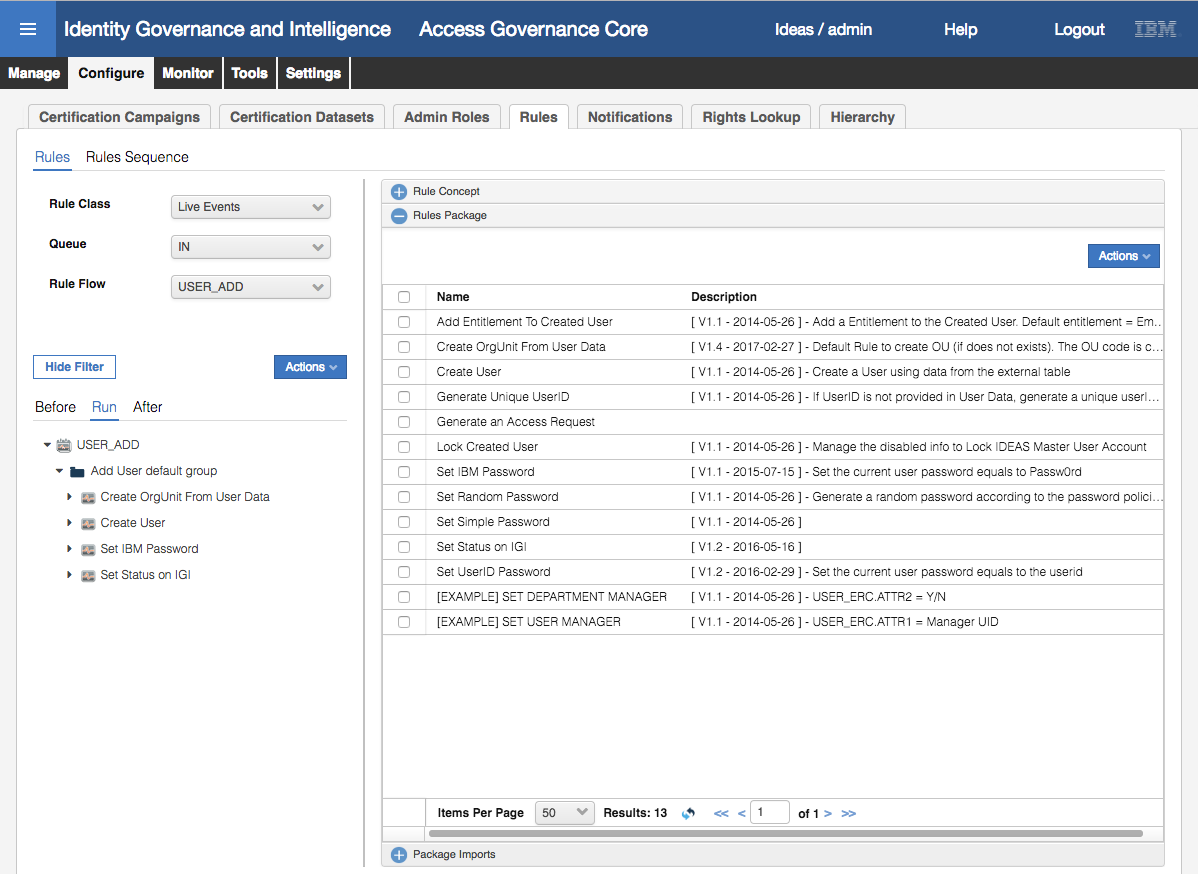
* Log into the **IGI Administration Console**, **Access Governance Core**
* Go to **Configure > Rules**
* Select the following; **Rule Class** = Live Events, **Queue** = IN, **Rule Flow** = USER\_ADD



* Expand the twisty and view the rules currently deployed as part of the User\_Add Rule Flow 

Note there are 4 rules deployed.

* Open the **Rules Package** slider in the right panel  and view all the available rules in the USER\_ADD package that are able to be deployed.



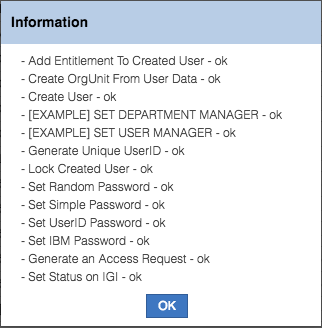
There are several rules in the package that can be added to the flow. These are supplied as examples of possible rule that can be deployed to react to a new user.

The rules in the configured rule flow execute in the descending order in which they are placed in the flow. The objects in memory are passed from rule to rule.

First, verify (compile) the rules in the package

* From the right panel, select **Actions > Verify**

View the results of the Verify



Notice that all the rules in the package are compiled, not just the one that are deployed as part of the rule flow.

* Click **OK** to close the Information dialog

### Creating a New Rule

This follow section creates a new rule for the package that sets a default expiration date for a new users IGI account. Through a workflow process initiated by a User Manager, it adds an Add\_User event to the Event IN Queue, triggering the Live Events🡪In🡪Rule Flow. The following is the pseudo design for the rule

Create the rule under Live Events/IN/USER\_ADD so include in the working memory (when clause) the objects needed in memory

The expiration date to set is for the IGI account (AccountBean) of the new hire, not in the user (UserBean)!

The IGI account of the new hire is the one having the Account Configuration «Pwdcfg» name «Ideas» or id «1». It’s a technical entry not deletable (all the users in the system must have this account)

The UserAction.findAccount(Dao sql, UserBean yourNewHire, AccountBean accountFilterForIdeasAccountOnly) method returns a list (BeanList) of the accounts of a user (UserBean) filtered by account (AccountBean)

Set the property «Expire» of the account and then save the AccountBean with the method UserAction.updateAccount(Dao sql, AccountBean theIdeasAccountOfNewHire)

Use Java Calendar class to define the date. Note: this is a Java class, not an IGI class. Rules can leverage the full power of Java and any package imported into the Rules package.

For test purpose set expiration date only 5 minutes after creation

Verify the new Rule

To meet this requirement, you could design the Java code from scratch, or used the supplied example shown below (cut and paste)

when

userBean : UserBean( ) // Get the user of the Add\_User

orgUnitBean : OrgUnitBean( ) // Get the org unit of the user

externalInfo : ExternalInfo( )

userErcBean : UserErcBean( )

then

logger.info("User to process : " + userBean.getCode()); // Log the user to be processed

AccountBean userAccount = new AccountBean();

userAccount.setPwdcfg\_id(1L); // IDEAS cfg, ID=1

// Search the users accounts and filter for the IGI account

BeanList accounts = UserAction.findAccount(sql, userBean, userAccount);

userAccount = (AccountBean) accounts.get(0);

// Expiration IGI account after 5 minutes

Calendar currentTime = Calendar.getInstance(); //Get the Current Time

currentTime.add(Calendar.MINUTE, 5); // Add 5 minute

Date newEntDate = currentTime.getTime(); //Set the new time

logger.info("Exp Date: " + newEntDate); // Log the expiration date/time

userAccount.setExpire(newEntDate); // Set the account expiration attribute

logger.info("Expiration Date set!!!!"); // Log that it set

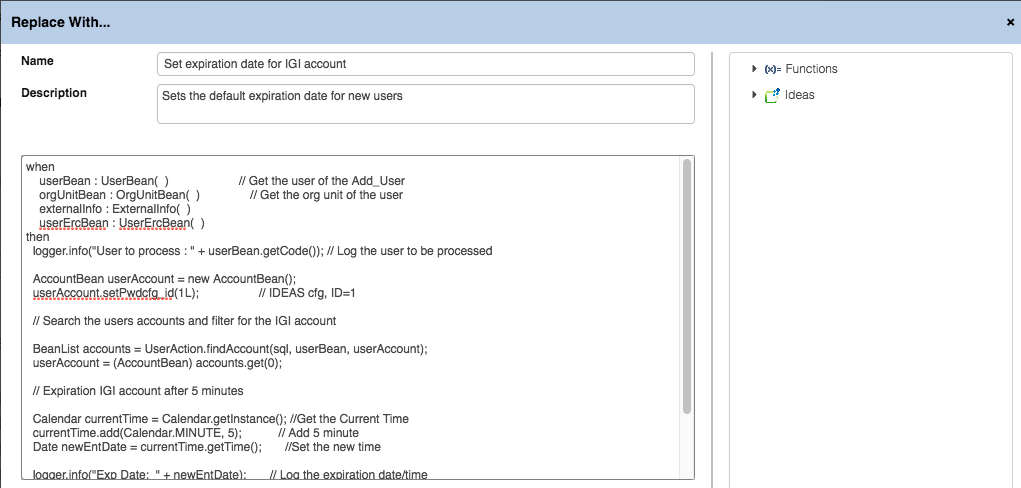
UserAction.updateAccount(sql, userAccount ); // Update the users IGI account

To create the new rule:

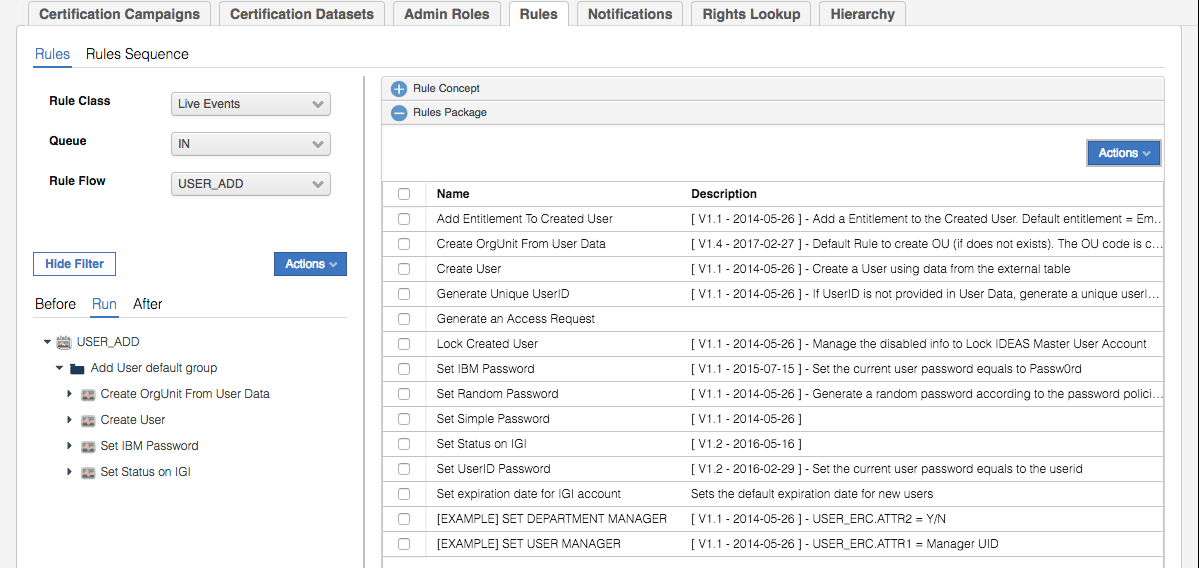
* From the right panel, in the Rules Package section, select **Actions > Create**

A new rule editing session pops up.

* On the Replace With… dialog, enter the following values:
* **Name** = “Set expiration date for IGI account”
* **Description** = “Sets the default expiration date for new users”
* Add the Java Code – either copy your own code in or copy’n’paste the code above into the field that currently has “when then”

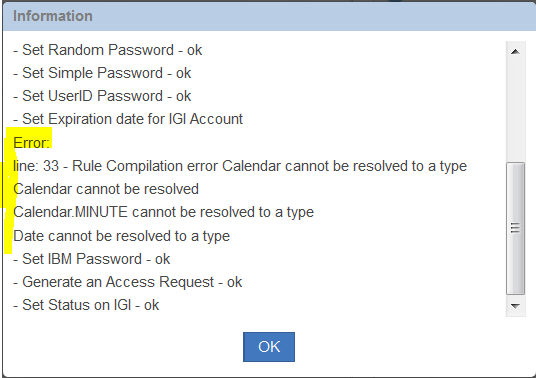


* Click **Save** to save the rule and close the Replace With… dialog



You may notice that the supplied rules include some version control in the description. This is purely arbitrary and not enforced or visible to the application. It would make sense to apply naming standards and version control to production deployments, particularly if multiple people are developing rules.

* From the right panel, select **Actions > Verify**
* View the results of the Verify



The verify for the new rule fails.

Error:

line: 33 - Rule Compilation error Calendar cannot be resolved to a type

Calendar cannot be resolved

Calendar.MINUTE cannot be resolved to a type

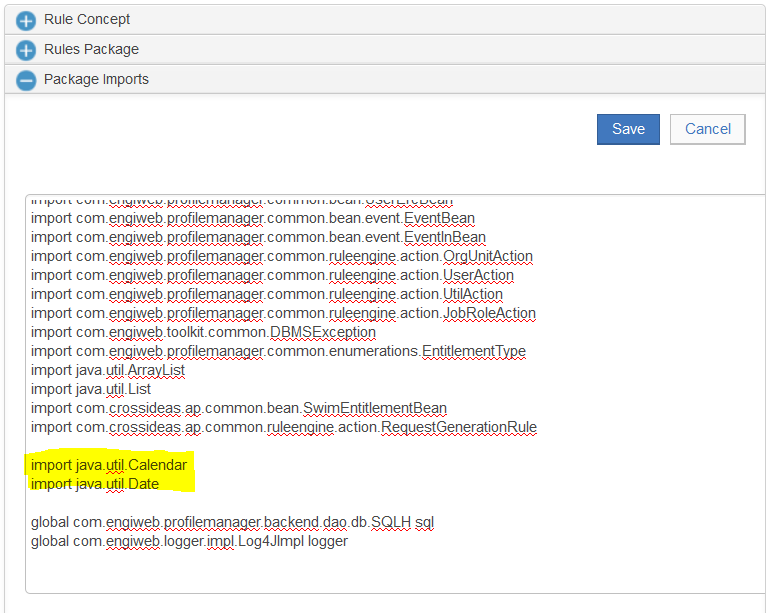
Date cannot be resolved to a type

The Java code uses two new classes to calculate the date and time of the account expiration. However, these classes were not in the list of packages imported for use by the rules in the rule flow. To correct this error, add the Java packages java.util.Calendar and java.util.Date to the package imports for the rule flow.

* Click **OK** to close the Information dialog
* Select the slider **Package Imports** 
* Add the following import statements

import java.util.Calendar

import java.util.Date



* Click **Save** to save the changes
* Verify the rules again. Note that all the rules compile “ok”

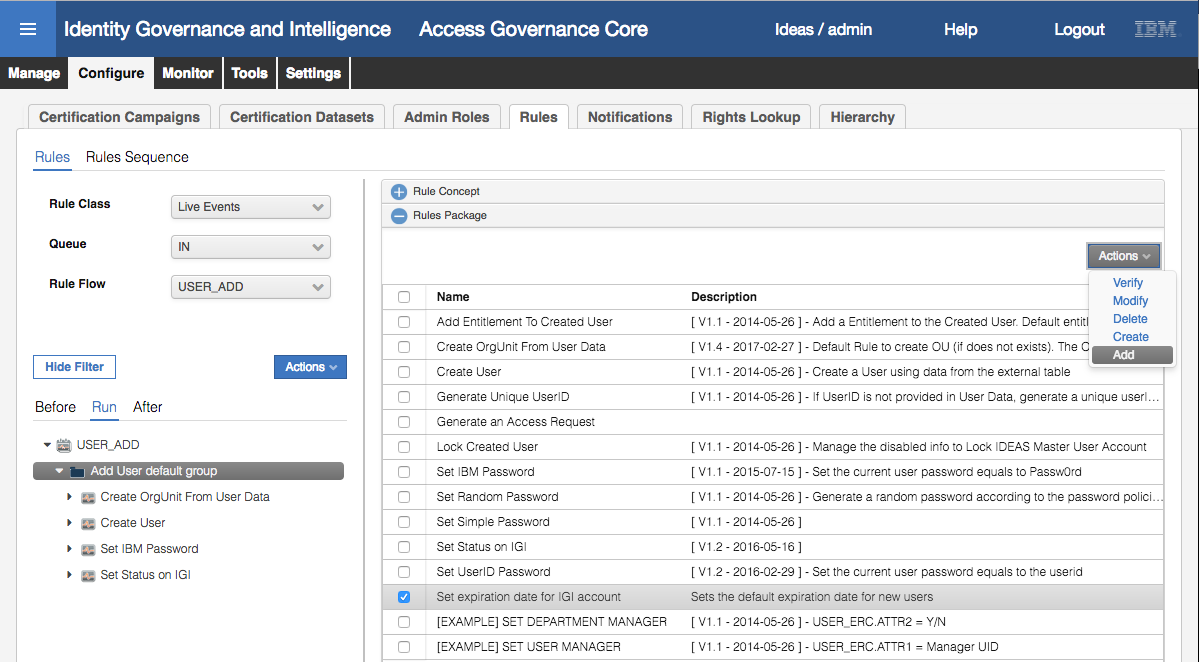
### Deploying the new rule as part of the rule flow

The new rule is ready for deployment into the rule flow

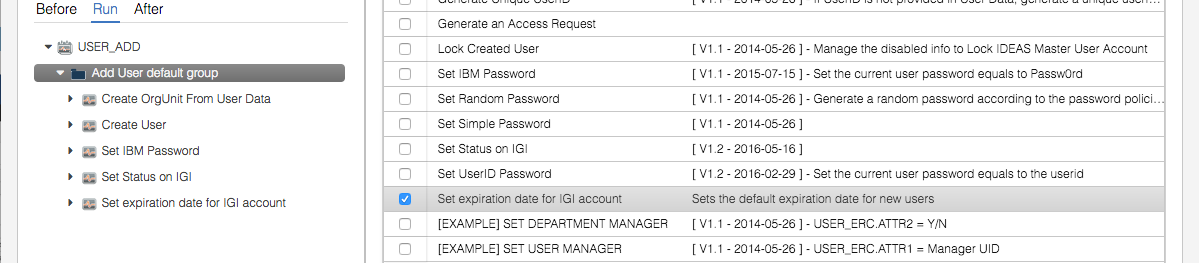
* In the right panel, expand the **Rules Package**
* Select the rule, “Set expiration date for IGI account”
* In left panel, highlight the group “Add User default group”
* In the right panel execute **Actions > Add**

The rule “Set expiration date for IGI account” is added to the end of the rule flow.

Before…



After…



The new rule will now execute when new users are created via a Service Center Process

## Create a new user using the “New Hire” process

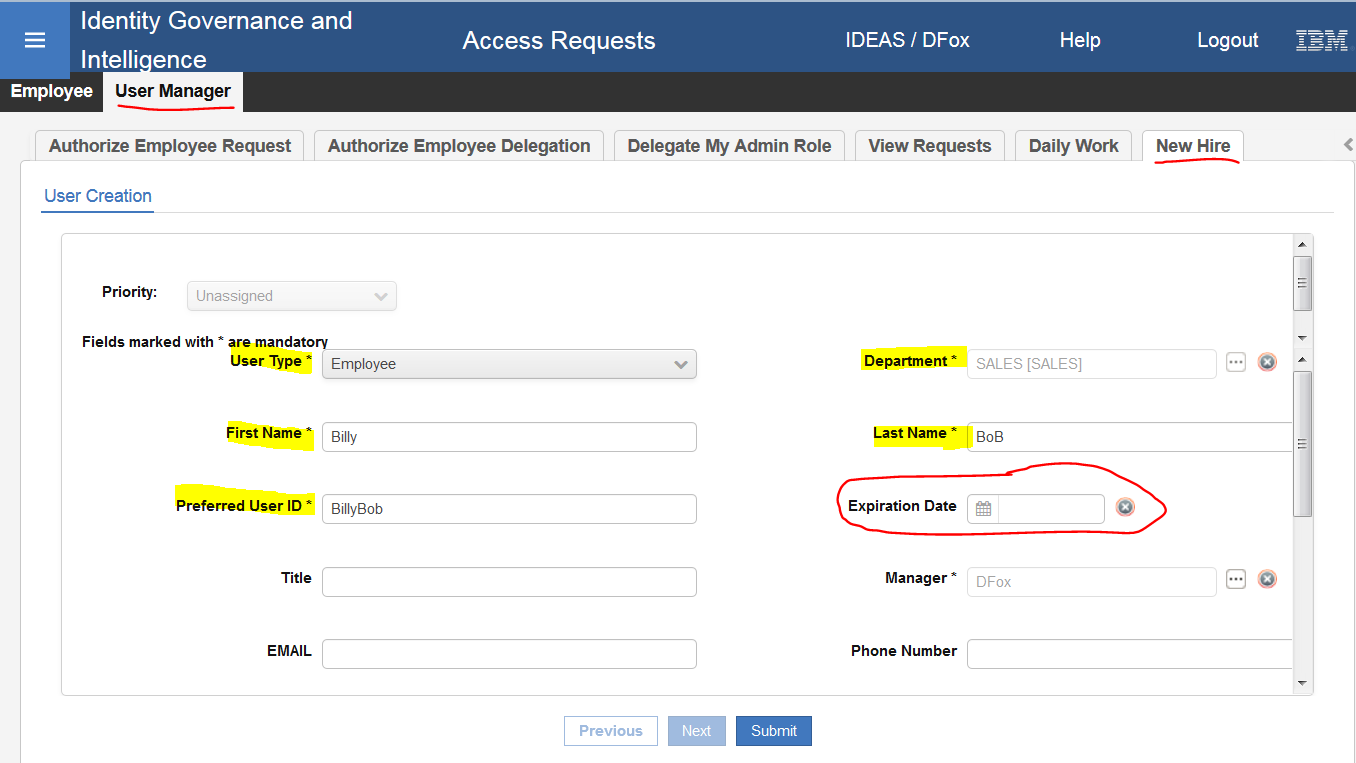
Test the new rule by creating a new user using the Service Center and verifying the Expiration date in the Admin Console.

### Manager creates and new user using the Service Center

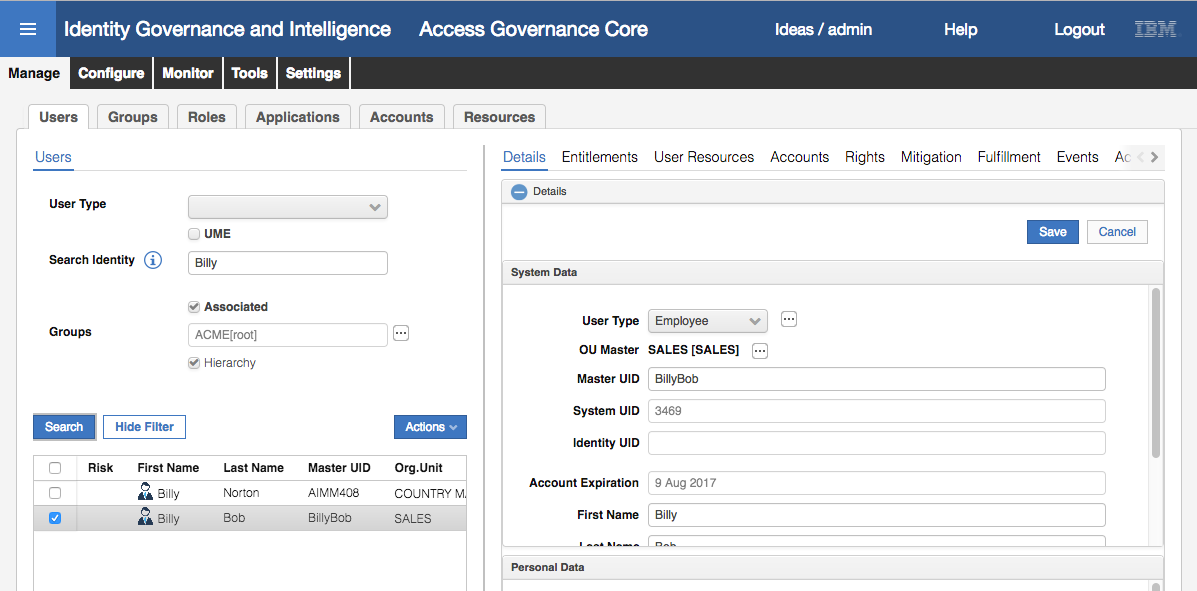
A manager logs in to the Service Center and acting as a User Manager completes the New Hire form to create a new user.

Follow the following steps:

* Open the **IGI Service Center** (DFox/Passw0rd)
* Use the main menu (“hamburger icon”) to go to **Access Requests**
* Choose the **User Manager** tab
* Choose the **New Hire** tab
* Fill out the following fields (most of the values are not important)
  + Choose **User Type** = Employee
  + Choose **Department** = Sales
  + Enter any **First Name**
  + Enter any **Last Name**
  + Set any **Preferred User ID**
  + Leave the **Expiration Date** empty
  + Choose **Manager** = Dfox
* Click **Submit**



* Click **OK** on the Request Submitted dialog
* Log out of the **Service Center**
* Open the **IGI Administrative Console** (admin/admin) and go to **Access Governance Core**
* Go to **Manage > Users** and **Filter** for the user just created (e.g.Billy)
* View the new users details. Notice the Account Expiration has a date of today, as determined by the new rule in the rule flow



The screenshot was captured on 9 Aug 2017, and the expiration date has been set to that date. This custom code has worked as expected.

This completes this lab.

Care should be taken with choosing the settings for the attribute-permissions. Of note:

* Setting an attribute-permission a not required will mean the entire account attribute can be removed. If you need to have a default setting, you should make the attribute required.
* Once an attribute-permission has been marked as required and the permission is assigned to a user, the permission cannot be removed from the user.

End of Document

# Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan, Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
2Z4A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

**COPYRIGHT LICENSE:**

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2017. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp 2017. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information at [ibm.com/legal/copytrade.shtml.](file:///D:\ISAM\templates\white%20paper\www.ibm.com\legal\copytrade.shtml)

**Statement of Good Security Practices**

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

© International Business Machines Corporation 2017

International Business Machines Corporation  
New Orchard Road Armonk, NY 10504

Produced in the United States of America 01-2016

All Rights Reserved

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.